

ЗАСТОСУВАННЯ МЕТОДУ ЕКСПЕРТНИХ ОЦІНОК ДО ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Юлія Ткач, Світлана Казмірчук, Дмитро Мехед, Володимир Базилевич

У статті висвітлено метод експертних оцінок та особливості його застосовування на прикладі оцінювання інформаційних ризиків вищого навчального закладу. Головна особливість цього методу полягає у тому, що він використовується у випадках, коли ускладнено знаходження розв'язку математичними методами. У зв'язку із недостатністю достовірної статичної інформації або взагалі її відсутністю щодо загроз інформаційній безпеці найбільш поширеним методом оцінювання інформаційних ризиків є метод експертних оцінок. Схематично представлено послідовності дій згідно з методом експертних оцінок: формулювання мети дослідження, вибір експертів та формування експертної групи, складання анкет, анкетування, обробка та аналіз експертних оцінок. Запропоновано статистичний інструментарій для обробки та аналізу отриманих результатів анкетування експертів.

Ключові слова: метод експертних оцінок, інформаційний ризик, вищий навчальний заклад.

Постановка проблеми. У результаті глобалізаційних процесів у економічній, інформацій, технологічній та інших сферах відбулося значне зростання складності усіх систем діяльності людини, як наслідок, значно збільшилась їх нестійкість та невизначеність.

Різні державні та недержавні інститути піддаються впливу зовнішніх та внутрішніх факторів, що може призвести до значних втрат. У зв'язку з цим актуальним стає широке впровадження у процедури управління різноманітними інститутами механізмів регулювання чутливості до подій ризику та обмеження викликаних ризиками втрат.

Інформація сьогодні є одним з ключових елементів будь-якого бізнесу. Вона є предметом купівлі-продажу. Тому захищеність інформаційних ресурсів стає складовою успішного розвитку будь-якого підприємства. Вищий навчальний заклад не виняток.

Таким чином, оцінювання інформаційних ризиків вищого навчального закладу є сьогодні надзвичайно актуальним.

Аналіз останніх досліджень і публікацій. Проблемою оцінювання інформаційних ризиків займаються такі науковці, як О.Є. Архіпов, С.Ф. Гончар, В.Б. Дудикевич, С.В. Казмірчук, О.Г. Корченко, Б.П. Томашевський. Ними досить різносторонньо висвітлено питання оцінки ризику. Незважаючи на значний обсяг накопичених у даній сфері знань, недостатньо дослідженим залишився статистичний аспект оцінювання інформаційних ризиків за допомогою методу експертних оцінок.

Мета статті є висвітлення особливостей застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу.

Виклад основного матеріалу. Існує багато різних тлумачень поняття «ризик». О.Г. Корченко у своїй статті [1] проаналізував та розкрив поняття ризику з його подальшою інтерпретацією у галузі інформаційної безпеки. Аналіз засвідчив, що різні тлумачення ризику мають спільну множину характеристик:

- ризик розглядається як ймовірність, що вимірюється або розраховується,
- ризик пов'язаний із настанням деякої події, як правило несприятливого,
- поняття ризику розкривається через діяльність суб'єкта,
- ризик розкривається через подію, яка не залежить від суб'єкта діяльності,
- акцент робиться на кількісну та кісну оцінку ризику,
- поняття ризику розкривається через невизначеність,
- ризик відображається ситуацією вибору з двох або з n варіантів відповідей,
- ризик сприймається як небезпека, частота, витрати або трати, характеристика ситуації, сумарна величина.

Зауважимо, що під час розкриття поняття ризику та при його оцінюванні необхідно обов'язково враховувати, що більшість подій та більшість рішень приймаються в умовах невизначеності.

Інформаційний ризик – це можливість настання випадкової події в інформаційній системі підприємства, що призводить до порушення її функціонування, зниження якості інформації нижче за допустимий рівень, у результаті чого підприємство зазнає збитків [3]. Але вважаємо, що подія може бути і не випадкова. Тобто, для вищого нав-

чального закладу інформаційний ризик – це невідомість, що може виникнути у результаті діяльності вузу, яка проявляється у неповноті, неточності, відсутності інформації та призводить до негативних наслідків [5].

Отже, оцінювання інформаційного ризику вищого навчального закладу – ідентифікація інформаційних активів, виявлення загроз та їх впливу на складові системи.

Для оцінювання інформаційного ризику використовуються різноманітні методи, методики та методології. Наприклад, статистичний та аналітичний методи, які розглянемо далі.

Аналітичний метод для оцінки ризику передбачає використання традиційних показників, які застосовуються при оцінці ефективності інвестиційних та інноваційних проектів: період окупності, внутрішня норма прибутковості, індекс рентабельності, чистий приведений дохід. Порівнюючи значення перерахованих показників альтернативних проектів, визначають їх ступінь ризику [2].

Статистичний метод - це розрахунок ймовірностей виникнення збитку на основі аналізу всіх статистичних даних, що є в наявності, які відносяться до результативності бізнесу у минулому.

Даний метод базується на аналізі коливань оціночного показника (величині втрат, що були допущені в минулих періодах господарської діяльності). Суть цього методу полягає в тому, що для розрахунку ймовірностей виникнення збитків аналізуються всі статистичні дані, що стосуються результативності здійснення фірмою розглянутих операцій. Останнім часом широко застосовується різновид даного методу – метод Монте-Карло, який за допомогою імітаційного аналізу дозволяє встановлювати ймовірності та величини змін оціночних характеристик проекту при можливому настанні несподіваних кризових ситуацій. Даний метод вимагає побудови і серйозних досліджень математичних моделей. Побудова моделі розпочинається з визначення функціональних залежностей у реальній системі, які згодом дозволяють одержати кількісне рішення, спираючись на теорію ймовірностей і генератор випадкових чисел. Застосування цього методу потребує спеціальної програмної підтримки [2].

Зазначимо, що статистичний метод можна використовувати у випадку наявності досить великої кількості даних про результати діяльності установи, для якої здійснюється аналіз.

У зв'язку із недостатністю достовірної статичної інформації або взагалі її відсутністю щодо загроз інформаційній безпеці, то найбільш поширеним методом оцінювання інформаційних ризиків є метод експертних оцінок.

Метод експертних оцінок – це евристичний метод, який застосовується у випадках, коли ускладнено знаходження розв'язку математичними методами.

Суть цього методу. Оцінка ризику виконується на основі суб'єктивних думок експертів-фахівців у конкретній галузі діяльності. Метод експертних оцінок полягає в тому, що команда проекту виділяє певну групу ризиків і розглядає, яким чином вони впливають на діяльність підприємства. Цей розгляд зводиться до подачі бальних оцінок за ймовірність виникнення того чи іншого виду ризику, а також ступеня його впливу на діяльність проекту [4].

Процес оцінювання ризиків передбачає визначення об'єкта дослідження.

Об'єктом нашого дослідження було обрано вищий навчальний заклад. Представимо схематично послідовність дій, згідно з методом експертних оцінок (рис. 1).

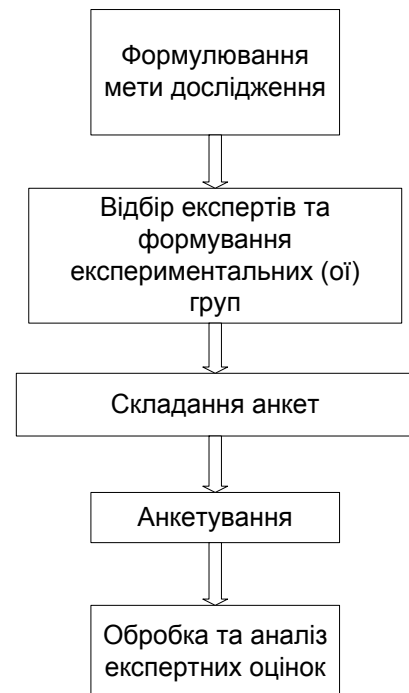


Рис. 1. Схема методу експертних оцінок

Метою нашого дослідження є визначення загроз інформаційній безпеці та оцінка їх сили впливу на функціонування вищого навчального закладу.

Здійснимо відбір експертів та сформуємо експертну групу.

Для відбору експертів треба визначити перелік критеріїв, яким мають відповідати експерти. Наприклад, повна вища технічна освіта, стаж роботи в сфері захисту інформації не менше 5 років або науковий ступінь кандидата (доктора) наук, вчене звання доцента (професора) тощо.

Ми відібрали експертів згідно з вище перерахованими критеріями, тому будемо вважати, що експерти є висококваліфікованими фахівцями у сфері інформаційної безпеки.

Зауважимо, що при цьому вони мають бути незалежними та незацікавленими у об'єкті, що досліджується, а саме не працювати на підприємствах, що конкурують, не приймати участь в діяльності установ, що здійснюють державний контроль даного підприємства і т.д.

Мінімальну кількість експертів ми визначити на основі статистичного підходу. Для цього використали загальноприйняту формулу для визначення мінімального обсягу вибірки:

$$N = \frac{t_{\alpha}^2 \cdot \sigma^2}{\Delta^2},$$

де t_{α} – довірче число, що залежить від ймовірності результату оцінювання, σ – середньо квадратичне відхилення, Δ – гранична похибка.

Тоді, для рівня значущості $\alpha = 0,05$ критерій $t_{\alpha} = 1,96$. Зауважимо, що це значення критерію t_{α} для невеликої вибірки, а саме до 30 одиниць.

Дисперсію визначимо як добуток $p \cdot q$, де p – доля одиниць, що володіють певною ознакою, а q – доля одиниць, що не володіють певною ознакою. Приймемо їх значення рівними 0,5 (оскільки цей показник відповідає найбільшій можливій варіації сукупності).

Для оцінки відносної граничної похибки нами було використано статистичне правило, що похибка не повинна перевищувати 5%.

Під час виставлення балів експертами можуть бути використані різні шкали, наприклад, п'ятибальна шкала Лайкерта (1-абсолютно неймовірно, 2 – неймовірно, 3 – не визначився, 4 – ймовірно, 5 – дуже ймовірно), або семибальний семантичний диференціал, або десятибальна шкала Степела (1-5 – ймовірність настання ризику незначна, 6-10 – найбільш ймовірний ризик).

Ми обрали десятибальну шкалу оцінювання, тобто експерти виставляти бали від 1 до 10. Тоді гранична похибка становила 0,5 балів.

Таким чином,

$$N = \frac{1,96^2 \cdot 0,5 \cdot 0,5}{0,5^2} \approx 4.$$

Отже, мінімальна кількість експертів в групі, за умови використання десятибальної шкали оцінювання, має становити 4 людини.

Зазначимо, що за умови обрання семибальної шкали мінімальна кількість експертів мала б становити 8 осіб, а п'ятибальної – 16.

Після формування експертної групи експертам було скласти перелік інформаційних ризиків, що можуть виникнути у вищому навчальному закладі. Список ризиків, визначених експертами, для вищого навчального закладу подано в таблиці 1.

Таблиця 1

Список інформаційних ризиків
для вищого навчального закладу

1.	Фальшування
2.	Розголошення конфіденційної або комерційної інформації
3.	Занесення вірусів
4.	Крадіжка
5.	Апаратні та програмні збої
6.	Халатність
7.	Саботаж
8.	Хакерські атаки

Далі експерти із запропонованого ними всіма переліку ризиків, що можуть виникати у сфері інформаційної безпеки вищого навчального закладу, визначити ті, які є найбільшій ймовірні, на їх думку, і ті ймовірність настання яких є меншою.

Сукупність відповідей експертів необхідно дослідити на нерівномірність.

Це можна зробити за допомогою таких статистичних показників:

1) середнє (\bar{x}) – покаже зведену (інтегровану) оцінку опитаних експертів,

2) стандартне відхилення (σ) – покаже зведене відхилення думки експертів від середніх значень (при цьому дане відхилення має бути в межах $\bar{x} \pm 3\sigma$),

3) коефіцієнт варіації ($V = \frac{\sigma}{M}$) – охарактеризує співвідношення середньоквадратичного відхилення та математичного сподівання (середнього), що покаже міру ризику притаманного досліджуваному явищу.

Обчислимо зазначені вище показники та запишемо отримані результати в таблиці 2.

Результати опитування групи експертів

Ризики	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Сума	Середня	Стандартне відхилення	Варіація
Фальшування	10	8	7	8	33	8,25	1,258306	0,152522
Розголошення конфіденційної або комерційної інформації	2	3	3	4	12	3	0,816497	0,272166
Занесення вірусів	4	2	3	3	12	3	0,816497	0,272166
Крадіжка	5	4	5	4	18	4,5	0,57735	0,1283
Апаратні та програмні збої	6	5	6	5	22	5,5	0,57735	0,104973
Халатність	7	9	8	7	31	7,75	0,957427	0,123539
Саботаж	3	4	4	3	14	3,5	0,57735	0,164957
Хакерські атаки	1	1	2	2	6	1,5	0,57735	0,3849

Щодо думок експертів, то зауважимо, що показник варіації засвідчить:

- 0-33% – сукупність однорідна, середня є типовою, варіація незначна,
- 34-66% – сукупність однорідна, середня є типовою, варіація значна,
- 67-100% – сукупність неоднорідна, середня не є типовою, варіація висока.

Отже, за високого або значного рівня варіативності за однією з груп досліджуваних ризиків спостерігається значна варіація, то це вказує на неспівставність відповідей експертів по заданому питанню і потребує вирішення у двох напрямках:

- 1) видалення одиниць, що деформують сукупність (усунути одного з експертів, чий відповіді найбільш неузгоджені із відповідями інших),
- 2) видалення досліджуваних факторів із переліку питань (видалення певного ризику з переліку або проведення додаткового дослідження із такими ризиками, але за участі інших експертів, оскільки у даному питанні сформована група експертів може виявитись некомпетентною).

У випадку незначної варіації, як у наведеній нами ситуації, можна говорити про співставність думок експертів щодо досліджуваного процесу.

Оцінимо міру узгодженості думок експертів.

Оскільки кількість ранжованих ознак (експертів) більша двох, то для оцінки міри узгодженості думок експертів використаємо коефіцієнт конкордації:

$$W = \frac{12 \sum_{j=1}^n d_j^2}{m^2(n^3 - n)},$$

де n – кількість факторів; m – кількість експертів; d_j – відхилення суми від середньої суми. При цьому

$$d_j = S_j - \frac{\sum_{j=1}^n S_j}{n},$$

де S_j – сума рангів.

Розрахунки наведено в таблиці 3.

Таблиця 3

Таблиця зведених розрахунків з оцінки узгодженості між думками експертів

	Експерт 1	Експерт 2	Експерт 3	Експерт 4	S_j	d_j
1	1	3	3	2	9	81
2	2	2	1	1	6	144
3	3	1	2	3	9	81
4	4	4	5	4	17	1
5	5	5	4	5	19	1
6	6	8	6	7	27	81
7	7	6	7	6	26	64
8	8	7	8	8	31	169
Сума					144	622
Середня					18	

Таким чином, коефіцієнт конкордації дорівнює:

$$W = 0,925595 \approx 0,93.$$

Коефіцієнт конкордації змінюється в межах від 0 до 1. Чим ближче коефіцієнт до одиниці, тим більший ступінь узгодженості думок експертів, і навпаки. У випадку, коли коефіцієнт конкордації дорівнює одиниці, то це означає, що всі експерти надали однакові ранги ризикам, якщо він дорівнює 0, то думки експертів не узгоджені. Зазвичай вважається, що думки експертів узгоджені, якщо $W \geq 0,7$. Отже, думки наших експертів дуже сильно узгоджуються одна з одною.

Разом з тим, розрахований нами коефіцієнт конкордації треба перевірити на статистичну значущість. Якщо кількість можливих ризиків, що пропонуються для оцінки експертам, більша за сім, то перевірити статистичну значущість коефіцієнта конкордації можна за допомогою критерію Пірсона ($\chi^2_{\text{розрах}}$), а якщо їх кількість менша семи, то за допомогою F - розподілу.

Для нашого прикладу, ми використали $\chi^2_{\text{розрах}}$. Він дорівнює 25,92.

Табличне значення $\chi^2_{\text{табл}} = 14,1$ при рівні значущості $\alpha = 0,05$ та ступенях вільності 7. Тобто розраховане нами значення перевищує табличне (критичне).

Таким чином, у нашому випадку значення коефіцієнта конкордації більш 0,7 та встановлено перевищення розрахункового значення критерію Персона над табличним, то ми можемо остаточно стверджувати про узгодженість думок експертів.

Після встановлення узгодженості думок експертів та її статистичної значущості варто визначити, у якій мірі кожний експерт впливає на узгодженість думок. Для цього потрібно послідовно, одного за одним, виключати з розрахунку експертів та обчислювати коефіцієнт конкордації, а також встановлювати його статистичну значущість. Це дасть можливість визначити експерта, який надавав найбільш неординарні відповіді. Але це не є приводом для його вилучення з експертної групи.

Також, отримані за допомогою методу експертних оцінок результати можна використати для кількісного оцінювання зон ризику закладу, що характеризують певний рівень можливих втрат. За міру ризику можна прийняти показник стандартного відхилення (σ). Загальноприйнято вважати, що прийнятним є ризик до 0,125, витратам у розмірі половини чистого прибутку відповідає коефі-

цієнт ризику від 0,125 до 0,25, у випадку, якщо ризик становить 0,25 і більше, то це свідчить про втрату усього чистого прибутку підприємства.

Висновки і пропозиції. Отже, метод експертних оцінок є дуже поширеним методом оцінювання інформаційного ризику, вищого навчального закладу зокрема. Результати опитувань експертів мають бути проаналізовані за допомогою різноманітного статистичного інструментарію. Обираючи інструментарій під час застосування методу експертних оцінок для оцінювання інформаційних ризиків вищого навчального закладу, треба враховувати різні фактори, а саме, мету дослідження, шкалу вимірювання відповідей експертів, кількість ризиків, які притаманні ВНЗ на думку експертів тощо.

Таким чином, можна отримати важливу для вищого навчального закладу інформацію щодо інформаційних загроз та вчасно вжити відповідні заходи.

ЛІТЕРАТУРА

- [1]. А. Корченко, В. Щербина, С. Казмирчук, "Методы анализа и оценки рисков потерь государственных информационных ресурсов" [Электронный ресурс]: Режим доступа: www.archive.nbu.gov.ua/portal/natural/Zi/2012_1/20.pdf.
- [2]. "Методи кількісного аналізу". [Електронний ресурс]. Режим доступу: <http://bibliograph.com.ua/economika-predpriyatiya-3/154.htm>.
- [3]. "Парадигма информационных рисков. Визначення". [Электронный ресурс]: Режим доступа: www.fa-kit.ru.
- [4]. "Проектні ризики та методи їх зменшення". [Електронний ресурс]. Режим доступу: www.info-works.com.ua/referats/finansi/5.html.
- [5]. Ю. Ткач, "Побудова нечітких когнітивних карт для оцінки інформаційних ризиків вищого навчального закладу", *Вісник Чернігівського державного технологічного університету. Серія «Технічні науки»: науковий збірник*, Чернігів: ЧНТУ, №2(73), С. 149-153, 2014.

REFERENCES

- [1]. A. Korchenko, "Methods of analysis and evaluation of the risks of loss of state information resources", 2012. [Online]. Available: www.archive.nbu.gov.ua/portal/natural/Zi/2012_1/20.pdf.
- [2]. "Methods for quantitative analysis", 2013. [Online]. Available: <http://bibliograph.com.ua/economika-predpriyatiya-3/154.htm>.
- [3]. "The paradigm of information risks", 2012. [Online]. Available: www.fa-kit.ru.
- [4]. "Project risks and methods of reducing", 2015. [Online]. Available: www.info-works.com.ua/referats/finansi/5.html.

- [5]. Іу. Tkach, "Construction of fuzzy cognitive maps for assessing information risks higher education institution", *Visnyk Chernihivskoho derzhavnogo tekhnolohichnogo universytetu. Seriya «Tekhnichni nauky»: naukovyi zbirnyk*, no.2(73), pp. 149-153, 2014.

ПРИМЕНЕНИЕ МЕТОДА ЭКСПЕРТНЫХ ОЦЕНОК К ОЦЕНКЕ ИНФОРМАЦИОННЫХ РИСКОВ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

В статье освещены метод экспертных оценок и особенности его применения на примере оценки информационных рисков вуза. Главная особенность этого метода заключается в том, что он используется в случаях, когда затруднено нахождения решения математическими методами. В связи с недостаточностью достоверной статической информации или вообще ее отсутствием относительно угроз информационной безопасности наиболее распространенным методом оценки информационных рисков является метод экспертных оценок. Схематически представлены последовательности действий по методу экспертных оценок: формулировка цели исследования, отбор экспертов и формирование экспертной группы, составление анкет, анкетирование, обработка и анализ экспертных оценок. Предложено статистический инструментарий для обработки и анализа полученных результатов анкетирования экспертов.

Ключевые слова: метод экспертных оценок, информационный риск, высшее учебное заведение.

APPLICATION OF THE EXPERT ASSESSMENT METHOD TO ASSESSMENT INFORMATION RISKS HIGHER EDUCATIONAL INSTITUTION

In the article the method of expert evaluations and especially its application as an example the evaluation of information risks of higher education. The main feature of this method is that it is used in cases where the solution of the complicated mathematical methods. Due to the lack of reliable information static or even its absence on information security threats, the most common method of risk assessment information is the method of expert evaluations. Schematically presented action sequences according to the method of expert ratings formulating research objectives, the selection of experts and the formation of a task force drafting questionnaires, surveys, processing and analysis of expert opinion. A statistical tools for processing and analysis of the results of questioning of experts.

Keywords: method of peer review, information risk, higher educational institution.

Ткач Юлія Миколаївна, к.п.н., доцент, завідувач кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.

E-mail: tkach_ym@ukr.net

Ткач Юлия Николаевна, к.п.н., доцент, заведующая кафедрой математического моделирования и информационной безопасности Черниговского национального технологического университета.

Tkach Yulia, PhD, associate professor, head of the department of mathematical simulation and information security, Chernihiv National University of Technology.

Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

E-mail: sv.kazmirchuk@gmail.com

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Мехед Дмитро Борисович, к.п.н., доцент кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.

E-mail: tkach_ym@ukr.net

Мехед Дмитрий Борисович, к.п.н., доцент кафедры математического моделирования и информационной безопасности Черниговского национального технологического университета.

Mekhed Dmitry, PhD, associate professor of mathematical simulation and information security department, Chernihiv National University of Technology.

Базилевич Володимир Маркович, старший викладач кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.

E-mail: tkach_ym@ukr.net

Базилевич Владимир Маркович, старший преподаватель кафедры математического моделирования и информационной безопасности Черниговского национального технологического университета.

Bazylevych Volodymyr, senior lecturer of mathematical simulation and information security department, Chernihiv National University of Technology.